UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

Pure Mathematics 429 — Cryptography – Design and Analysis of Cryptosystems

(see Course Descriptions under the year applicable: http://www.ucalgary.ca/pubs/calendar/)

Syllabus

Topics	**Number of hours**
Review of Basic Algorithms and Complexity: The Big O notation and its properties. Computational complexity. Applications to the Euclidean algorithm. Extended Euclidean algorithm. Half-Extended Euclidean Algorithm, modular inverses. Lamé's Theorem, computational complexity of the GCD, and the Least Absolute Remainder Algorithm. Exponentiation and its complexity. Polynomial arithmetic, Finite Field arithmetic and complexity. Constructing Finite Fields.	6
Discrete Logarithm Based Cryptography: Brief review of discrete logarithm based public key cryptography and signature schemes. Diffie-Hellman key exchange protocol. The Discrete Logarithm Problem in finite fields, its relevance to DLP based cryptosystems/protocols (ElGamal public key system, ElGamal Signature Scheme, Digital Signature Algorithm). Generalized Diffie-Hellman key exchange in finite groups. Baby step giant step algorithm for computing discrete logs and its complexity. Pollard-rho and Pollard Kangaroo methods. Pohlig-Hellman algorithm.	9
Factoring Based Cryptography: Brief review of factoring based public key dryptography and signature schemes. Review of RSA. Fast Decryption for RSA and its complexity/cost savings. Variants of RSA. The Integer Factoring Problem and its relevance to RSA. Smooth numbers, Pollard's p-1 Algorithm, the p+1 algorithm, Dixon's Factorization Method and the Quadratic Sieve. Complexity of these algorithms.	6
Primality Testing and Prime Generation: True primality tests, proofs via converse of Fermat's Little Theorem and their complexity. Probabilistic primality test, pseudo-primes, strong pseudo-primes. Quadratic reciprocity, Jacobi and Legendre symbols. Solovay Strassen Test, Miller-Rabin-Selfridge Test. Prime number Theorem and method for generating primes (and complexity).	6
Elliptic curves and cryptography: Introduction to Elliptic Curves over $\mathbb{Q}$ and over Finite Fields. Elliptic Curve Cryptography. Complexity of the Elliptic Curve Discrete Logarithm Problem, security considerations. Comparison of public-key cryptosystems via NIST recommendations.	6
TOTAL HOURS	**33**

Additional Topics (if time permits):

Knapsack: The subset sum problem, the knapsack problem, superincreasing sequences. Merkle-Hellman knapsack cryptosystem, Chor-Rivest knapsack cryptosystem. Discussion of the complexity of knapsack systems and explanation of how they were broken.

Zero-knowledge: Bit commitment revisited. Interactive minimum disclosure proof systems. Zero-knowledge proofs of knowledge, computational and perfect zero-knowledge. Feige-Fiat-Shamir identification protocol, cut and choose protocol-cave analogy, zero-knowledge proofs via Hamiltonian cycles, basic zero-knowledge noninteractive protocol, and zero-knowledge proof of discrete logarithm.

Quantum Cryptography: Heisenberg's uncertainty principle, quantum key generation, and a brief discussion of the future implications.

One-Way Functions and Hash Functions: Review of one-way functions. Coin Flipping by telephone using one-way functions (such as exponentiation). Bit commitment using symmetric-key cryptography. Hash functions and their applications. One-way hash functions and compression, iterated hash functions, unkeyed hash functions, hash functions based on modular arithmetic. Speedy stream cipher MAC. Attacks on hash functions.

* * * * * * *

2010:08:12 Effective Fall 2010
RS:jml
Description Change: 2011:07:01
WEC

PMAT 429 Cryptography — Design and Analysis of Cryptosystems
Course Outcomes

The main objective of this course is to provide a treatment of number theory as the foundation of public-key cryptography. Students will develop a solid understanding of number-theoretic algorithms and the ability to analyze their efficiency and complexity in the context of cryptology. In particular, a student who successfully completes this course will be able to:

1. Analyze the efficiency of basic algorithms used in cryptography, both in terms of run-time and storage.

2. Apply number theoretic algorithms and concepts to cryptanalyze public-key cryptographic primitives.

3. Demonstrate competence with algorithms for integer factorization, solving discrete logarithm problems, primality testing and elliptic curves.

4. Restate the main cryptographic protocols that are covered in the course and their different functions

5. Use mathematical reasoning to rigorously prove security, efficiency, and correctness of various cryptographic primitives.

6. Apply complexity results for number theoretic algorithms to determine appropriate parameter selection, security assessment, and efficiency of public-key cryptographic primitives.

* * * * * * *

2017/11/09
RJS
Course outcomes added